

# Index

## A

- accounts 254**
  - contract account (CA) 255
  - externally owned account (EOA) 254, 255
- account state 268**
  - balance 268
  - code hash 268
  - nonce 268
  - storage root 268
- account storage trie 268**
- active replication 120**
- actuators 716**
- address data type 362**
- advanced Bitcoin addresses 163**
- Advanced Encryption Standard (AES) 71, 74**
  - AddRoundKey 75
  - DES 74
  - for decryption 76, 77
  - for encryption 76, 77
  - MixColumns 75
  - ShiftRows 75
  - state 74
  - SubBytes 75
  - working 74, 75
- advanced protocols, Bitcoin 202**
  - Bitcoin Cash 204
  - Bitcoin Gold 205
  - Bitcoin Unlimited 205
  - Segregated Witness 202-204
  - Taproot 205, 206
- AES-128-CTR 252, 253**
- Agent 670**
- aggregate signatures 108**
- aggregation based oracles 237**
- AI 740**
- airdrop hunting 631**
- algocracy 44**
- Algorand 118**
- altcoin 208**
  - providing 209
- Amazon Web Services (AWS) 233**
  - reference link 514
- American National Standards Institute (ANSI) 530**
- Analog-to-Digital Converter (ADC) 718**
- analysis and design, consensus algorithm 122**
  - model 122
  - processes 122
  - timing assumptions 123
- Android proof 234**
- anonymity phase 591**
- Anonymous Credentials (AnonCreds) 444, 447, 675**
- Anti-Money Laundering (AML) 22, 744**
- Apache Camel 508**

- app.js JavaScript file**
  - creating 384-386
- Application Binary Interface (ABI) 346, 729**
- Application-Specific Integrated Circuits (ASICs) 185, 742**
- arbitrum 575**
- architecture development method (ADM) 511**
  - phases 512, 513
- argument of knowledge 603**
- arguments (AR) 598**
- Aries 444, 446, 675**
  - reference link 446
- arrays 363**
- Artificially Intelligent Decentralized Autonomous Organizations (AIDAOs) 741**
- asset classes 683**
- asset tokenization 694**
- associative 80**
- asymmetric cryptography 80**
  - blockchain technology 109
  - commitment schemes 110
  - encoding schemes 116
  - homomorphic encryption 109
  - integrated encryption scheme (IES) 83
  - private key 80, 81
  - public key 81, 82
  - secret sharing 109
  - verifiable random function (VRF) 117
  - zero-knowledge proofs (ZKPs) 111-113
- asymmetric cryptography algorithms 82**
  - discrete logarithm scheme 82
  - elliptic curves algorithm 83
  - integer factorization schemes 82
- atomic broadcast 121**
- atomic swaps 589**
- attacking hash functions**
  - birthday attack 636
  - collision attack 636
  - length extension attack 636
  - preimage attack 636
- attacks, on cryptocurrency wallets**
  - malware attacks 632
  - Man-in-the-Middle attacks 632
  - phishing attacks 632
  - security vulnerabilities, in cryptocurrency wallet code 633
- attacks, on hardware wallets**
  - malware attacks 633
  - Man-in-the-Middle attacks 633
  - physical tampering 633
  - supply chain attacks 633
  - user-level attacks 633
- attacks, on layer 2 blockchains**
  - attacks, on rollup provider 634
  - blockchain bridge-related vulnerabilities 634
  - data availability attacks 634
  - DSL bugs 635
  - state channels and side chain-related attacks 635
  - transaction censoring 634
- attack trees 647**
- attribute-based encryption (ABE) 593**
- Augur**
  - reference link 238
- automatable 224**
- Automated Market Maker (AMM) 696**
  - pros and cons 700
- Autonomous Agents (AAs) 42, 740**
- avalanche effect 57**
- Aztec 576**
  - URL 594
- Azure**
  - reference link 514

**B**

**bad randomness** 630

**Bankers' Automated Clearing System (BACS)**  
688

**base** 576

**base58-encoding scheme** 117

**base64-encoding scheme** 117

**Basecoin**

URL 475

**Beacon Chain** 409, 410

beacon node 410

consensus client 411

execution client 411

features 410

proof-of-stake 415-421

validator client 411, 412

**Beacon Chain nodes**

versus validator nodes 414

**beacon client** 418

**beacon node** 410

**Bech32 mechanism** 203

reference link 203

**Besu** 444, 446

reference link 446

**BFT algorithms** 129

HotStuff 151-155

Istanbul Byzantine Fault Tolerance  
(IBFT) 134-137

Nakamoto consensus 144

PoW 146

Practical Byzantine Fault Tolerance  
(PBFT) 129-131

Tendermint 137-141

**BigchainDB** 736

**binary signing** 745

**binding** 592

**biometric passports** 735

**BIP37** 193

**birthday attack** 636

**Bitcoin** 9, 157, 158, 715

advanced protocols 202

altcoin 208

core client and associated tools 209

cryptographic keys 159

extended protocols 206

innovation 200

in real world 197, 198

payments 198-200

reference link 622

**Bitcoin addresses** 161

advanced Bitcoin addresses 163

typical Bitcoin addresses 161-163

**Bitcoin APIs**

URL 219

**Bitcoin blockchain** 176

achieving, techniques 585

data structure 176-178

fork 179, 180

genesis block 178

orphan block 179

properties 180

stale block 179

**Bitcoin blockchain, techniques**

anonymous signatures 593

attribute-based encryption (ABE) 593

CoinSwap 589

confidential transactions 592

Dandelion 590-592

homomorphic encryption 587

I2P 586

Indistinguishable obfuscation (IO) 586, 587

Layer 2 protocols, using 594

MimbleWimble 592

mixing protocol 588, 589

privacy managers 594

secure multiparty computation 587

- Tor 586
- trusted hardware-assisted confidentiality 587
- TumbleBit 590
- Zether 594
- Zkledger 593
- Bitcoin Cash (BCH) 204**
  - reference link 204
- bitcoin-cli 210**
  - Bitcoin command-line tool, using 216
  - working with 214-216
- Bitcoin client installation 209**
  - bitcoin.conf, setting up 211
  - Bitcoin node, setting up 210
  - node, starting up in regtest 212-214
  - node, starting up in testnet 211, 212
  - source code, setting up 210
- Bitcoin command-line tool**
  - using 216
- Bitcoin core client 209**
  - bitcoin-cli 210
  - bitcoind 209
  - bitcoin-qt 210
  - download link 209
- Bitcoin Core software**
  - reference link 210
- Bitcoin, cryptographic keys**
  - private keys 159, 160
  - public keys 160
- Bitcoin futures**
  - reference 158
- Bitcoin Gold 205**
  - reference link 205
- Bitcoin Improvement Proposals (BIPs) 201, 552**
  - informational BIP 201
  - Payment 201
  - PaymentACK 201
  - PaymentRequest 201
  - process BIP 201
  - standard BIP 201
- Bitcoinj**
  - URL 219
- Bitcoin Lightning 557**
- Bitcoin merchant solutions**
  - URL 200
- Bitcoin miner 181, 182**
  - mining pool 186
  - mining systems 184
  - Proof of Work (PoW) 182-184
  - tasks, performing 181, 182
- Bitcoin miner, mining systems**
  - ASICs 185
  - CPU mining 184
  - Field Programmable Gate Arrays (FPGAs) 185
  - GPU 184
- Bitcoin network 186, 187**
  - bloom filter 192, 193
  - client software 192
  - protocol messages, types 187-191
- Bitcoin-NG 554**
  - microblocks 554
- Bitcoin programming 219**
- Bitcoin testnet**
  - reference link 191
- Bitcoin transactions 163, 164, 588**
  - bugs 175, 176
  - coinbase transactions 164, 165
  - data structure 167-169
  - elements 164
  - lifecycle 165, 166
  - Script language 170, 171
- Bitcoin transactions, data structure**
  - input (vin) 169
  - metadata 169
  - outputs (vout) 170
  - verification 170
- Bitcoin transactions, lifecycle**
  - fees 166, 167
  - validation 166

**Bitcoin transactions, Script language**

- contracts 174, 175
- opcodes 171
- standard transaction scripts 171-174

**Bitcoin Unlimited 205**

- reference link 205

**Bitcoin wallets 194**

- brain wallets 195
- deterministic wallets 194
- hardware wallets 195
- hierarchical deterministic wallets 194
- mobile wallets 195
- non-deterministic wallets 194
- online wallets 195
- paper wallets 195
- types 194

**BitDNS 715****BitPay**

- URL 200, 219

**Bitswap mechanism 39****Blake hash function**

- reference link 287

**blind signatures 10, 104**

- reference link 105

**blob-carrying transaction 434****blob transaction**

- lifecycle 434

**block-based DAGs 555****blockchain 11**

- and AI 740, 741
- append-only 11
- architecture 12
- as layer 12-14
- benefits and features 20, 21
- challenges 743-745
- compatibility, checking for enterprise 498
- distributed ledgers 11, 23
- emerging trends 741-743

- fully private and proprietary blockchains 25

- functioning 18, 19

- generic elements 14-18

- high-profile successful attacks 620

- history 8, 9

- in business 14

- layer 1 blockchain 26

- layer 2 blockchain 26

- Layman's definition 11

- peer-to-peer (P2P) 11

- permissioned ledger 25

- private blockchains 24

- public blockchain 24

- querying, with Geth 301

- security 619-621

- semi-private blockchains 24

- shared ledger 24

- technical definition 11

- tokenized blockchains 25

- tokenless blockchains 25

- types 23

- updatable via consensus 12

**blockchain, and IoT convergence**

- benefits 719-721

**blockchain application layer 628**

- DeFi attacks 631

- smart contract vulnerabilities 628, 629

**Blockchain as a Service (BaaS) 505, 513, 742**

- providers 514

**blockchain, as layer**

- Applications layer 14

- Consensus layer 14

- Cryptography layer 13

- Execution layer 14

- Network layer 13

**blockchain-based IoT implementation 722**

- electronic circuit, building 728, 729

- first node, setting up 725

- Node.js, installing 727, 728

- prerequisite hardware components 722
- Raspberry Pi node, setting up 726, 727
- Raspberry Pi, setting up 723-725
- Solidity contract, developing 729-733
- Solidity contract, running 734
- blockchain in finance, applications 685**
  - financial crime prevention 686-688
  - insurance industry 685
  - payment 688, 689
  - post-trade settlement 685
- blockchain.info**
  - URL 219
- blockchain layer 624**
  - attacks, on consensus protocols 626
  - attacks, on transactions 624, 625
  - chain reorganization 627
  - double-spending 627
  - forking 627
  - selfish mining attack 627
  - transaction replay attacks 625, 626
- blockchain layers**
  - blockchain application layer 621, 628
  - blockchain protocol layer 621, 624
  - cryptography layer 621
  - hardware layer 621-623
  - interface layer 621, 631
  - network layer 621-624
- Blockchain Open Ledger Operating System (BOLOS) 234**
- Blockchain oracle problem 235, 238**
- blockchain oracles**
  - services 239, 240
  - types 236
- blockchain oracles, types**
  - cryptoeconomic oracles 239
  - inbound oracles 236
  - outbound oracles 238, 239
- blockchain privacy 583**
  - anonymity 584
  - confidentiality 584
  - example 610-616
  - Zero-knowledge, using 594, 595
- blockchain privacy, zero-knowledge protocols**
  - cryptographic commitment 595-597
  - proofs 597-601
  - ZK-SNARKs, building 601-607
- blockchain services, Fabric 454**
  - consensus service 454
  - distributed ledger 455
  - ledger storage 456
  - peer-to-peer protocol 455
- blockchain solution**
  - implementation strategy, establishing 498
- blockchain technology**
  - growth 1-4
  - limitation 23
  - limitations 21, 22
- blockchain trilemma 546, 547**
  - properties 546
- blockchain, use cases 715, 716**
  - government 735
  - health 738, 739
  - IoT 716
  - media 739
- blockchain, using Geth**
  - interacting, methods 301
- Blockchain wallet**
  - using 198
- block cipher encryption function 73**
- block ciphers 71**
  - operation 72
- blockcracy 44**
- block data (transactions) 455**
- block encryption modes 72**
  - cipher block chaining (CBC) mode 72
  - counter (CTR) mode 72
  - electronic code book (ECB) 72

- keystream generation mode 73
- message authentication mode 73
- block headers** 275, 455
  - elements 275
- block interval reduction** 553
- block.io**
  - URL 219
- block-less DAGs** 555
- block metadata** 455
- block propagation** 553
- blocks** 274, 444
- block size**
  - increasing 552
- bloom filter** 192, 193
- bloXroute** 551
- BLS cryptography** 422
- Bluetooth Low Energy (BLE)** 40
- Blum-Blum-Shub (BBS)** 55
- Boba Network** 576
- Boneh-Lynn-Shacham (BLS)** 417, 422
  - aggregate signatures, reference link 108
- Boolean** 361
- boot nodes** 282
- brain wallets** 195
- Breadboard** 722
- bridgefy** 40
- Brownie** 352
  - reference link 352
- brute-force attack** 635
- btcd**
  - reference link 210
- BTC Relay**
  - URL 208
- bulletproofs** 598
- Byzantine Fault Tolerance (BFT)** 122, 501
- Byzantine Generals problem** 5

- Byzantine node** 741

- Byzantium** 281, 348

## C

- Cakeshop**

- transaction, viewing 538

- Caliper** 444, 448

- reference link 448

- Capital Gains Tax (CGT)** 743

- CAP theorem** 6, 7

- availability 6

- consistency 6

- partition tolerance 6

- carbon footprint, Bitcoin**

- reference link 147

- Cardano Ouroboros** 118

- Casascius physical bitcoins** 159

- Casper** 295

- reference link 281

- Casper the Friendly Finality Gadget (Casper-FFG)** 420, 429

- Cello** 444, 448

- reference link 448

- central bank digital currency (CBDC)** 22, 34

- Centralized Exchange (CEX)** 695

- versus DEX 700, 701

- Centralized Finance (CeFi)** 690

- centralized identity model** 652, 653

- centralized system** 30

- versus decentralized system 33

- Central Limit Order Book (CLOB)** 698

- Certificate Authority (CA)** 454, 458, 657

- certificates** 732

- certificates, PBFT** 131

- CFT algorithms** 124

- Paxos 124-127

- Raft 127-129

- chain-based PoS** 149
- chaincode** 450, 452
  - implementing 460, 461
- chained hashing scheme** 147
- chainlink**
  - URL 239
- chain of blocks** 11
- chain reorganization** 627
- Chain Virtual Machine (CVM)** 17
- challenge-response protocols** 82
- challenges, enterprise blockchain**
  - business challenges 518
  - compliance 518
  - interoperability 517
  - lack of standardization 517
- channels, Fabric** 457
- checkpointing** 133
- Chicago Mercantile Exchange (CME)** 157
- cipher block chaining mode (CBC mode)** 73
- cipher feedback (CFB) mode** 74
- ciphers** 52
- Clearing House Automated Payment System (CHAPS)** 688
- clients, Fabric** 457
- client software** 192
- Clique** 531
- closure** 80
- CNexchange (CNEX)** 480
- Cockpit** 352
- code signing** 745
- coin** 473
- coinjoin** 588
- CoinSwap** 589
- collision attack** 636
- collision resistance** 56
- colored coins** 206
- command-line interface (CLI)** 372
- commit chains** 559
- commitment schemes** 110, 111
  - commit phase 110
  - open phase 110
  - Pedersen commitment scheme 111
- commit phase** 110
  - binding property 110
  - hiding property 110
- committee-based PoS** 150
- committing peers** 457
- CommonAccord**
  - URL 228
- common language for augmented contract knowledge (CLACK)** 229
- common reference string model** 599
- Common Vulnerability Scoring System (CVSS)** 647
- compliance** 503, 504
- component requisites, private net**
  - data directory 285
  - genesis file 285
  - network ID 284
- computation oracles** 237
- Computation Tree Logic (CTL)** 642
- conditional privacy** 584
- confidentiality** 502
- confidential transactions** 592
- confusion property** 71
- consensus** 119
- consensus algorithm**
  - analysis and design 122
  - fundamental requirements 124
  - lottery-based 123
  - traditional voting-based 123



**consensus algorithm, selecting factors 155**

- finality 155
- performance 156
- scalability 156
- speed 156

**consensus client 411, 423****consensus layer 298****consensus mechanism 643, 644****consensus mechanism, Ethereum 279, 280****consensus protocol 17, 18****consensus service 454****consensus states, IBFT**

- committed 136
- final committed 136
- new round 136
- prepared 136
- pre-prepared 136
- round change 136

**consortium chain type 497****Constant Function Market Makers (CFMMs) 700****constant mean market makers (CMMM) 698****constant product market maker (CPMM) 697****Constant sum market makers (CSMM) 697****Constellation 524****constructor function 358****contest-driven decentralization 34****contract**

- functions, calling 388

**contract account (CA) 255**

- properties 255

**contract creation transactions 258, 264****contracts 174**

- compiling, with Truffle 393-397
- deploying 372-376
- interacting with 398, 399
- interacting with, via frontends 381, 382
- migrating, with Truffle 393-397

- querying, with Geth 377-380

- solc, used for generating ABI and code 376, 377

- testing, with Truffle 393-397

- Truffle, installing and initializing 392, 393

- Truffle, used for deploying and interacting with 391, 392

- Web3 and Geth, used for interacting with 371, 372

**contracts, via frontends**

- app.js JavaScript file, creating 384-386

- frontend webpage, creating 387-391

- functions, calling 388

- web3.js JavaScript library, installing 382, 383

- web3 object, creating 383

**control structures, Solidity 365, 366****Coq**

- URL 640

**Corda**

- reference link 24

**Counter Financing of Terrorism (CFT) 22****counterparty 207, 208**

- armory\_utxsrv 207

- counter block 207

- counter wallet 207

- server 207

- URL 208

**Counterparty coins (XCPs) 207****CPU-bound PoW 146****CPU mining 184****Crash Fault Tolerance (CFT) 120, 122, 467****cross link 410****crowd wisdom-driven oracles 237, 238****cryptocurrency 250****cryptoeconomic oracles 239****cryptographic commitments 595-597****cryptographic hash function applications 63**

- distributed hash tables 66, 67

- Merkle Patricia trie 65, 66
- Merkle tree 64
- cryptographic hash mode 73**
- cryptographic primitives 54, 55**
  - keyless primitives 55
  - symmetric key primitives 67, 68
  - taxonomy 54
- cryptography 52, 622**
  - accountability 54
  - non-repudiation 53
  - services 52-54
- cryptography layer**
  - attacking hash functions 636
  - key management-related vulnerabilities and attacks 636
  - public key cryptography, attacking 635, 636
  - ZKP-related attacks 637, 638
- cryptography, services**
  - authentication 53
  - confidentiality 52
  - data origin authentication 53
  - entity authentication 53
  - integrity 52
  - multi-factor authentication 53
- cryptojacking 622, 633**
- CryptoKitties 474, 480**
  - URL 474
- crypto malware 622**
- CryptoNote 109**
- crypto service provider, Fabric 459**
- CureCoin 739**
  - URL 739
- curl 218**
  - reference link 218, 303
  - URL 381
- cyclic group 80, 93**

## D

- DAG-based chains 554**
  - block-based DAGs 555
  - block-less DAGs 555
  - types 555
- Dagger 312**
- DAI 45**
  - URL 45
- Dai stable coin**
  - URL 475
- DAML 521**
  - reference link 522
- Dandelion protocol 590-592**
- danksharding 432**
- DAO hack 643**
- DAO legality**
  - reference link 48
- DApps stats**
  - reference link 46
- dark web 744**
  - reference link 744
- data availability 634      Data Availability Sampling (DAS) 433**
- Data Encryption Standard (DES) 71, 74**
- data integrity service 56**
- data types, Solidity**
  - reference types 361, 363
  - value types 361
- decentralization 29-33**
  - benefits 36, 37
  - contest-driven decentralization 34
  - disintermediation 33
  - methods 33
  - quantifying 34, 35
  - requirements evaluating 37, 38

- trends 48
- working 42
- decentralized applications (DApps) 44, 46, 230, 248, 471**
  - criteria 46
  - design 46-48
  - operations 46
  - Type 1 44
  - Type 2 45
  - Type 3 45
- decentralized autonomous corporation (DAC) 43**
- decentralized autonomous initial coin offering (DAICO) 478**
- Decentralized Autonomous Organizations (DAOs) 3, 43, 241, 242, 250, 478, 692, 693**
- decentralized autonomous society (DAS) 44**
- decentralized consensus 31**
- Decentralized Exchange (DEX) 695-697**
  - aggregator 699, 700
  - AMM, pros and cons 700
  - CMMM 698
  - CPMM 697
  - CSMM 697
  - order book-based DEX 698
  - versus CEX 700, 701
- decentralized finance (DeFi) 2, 690, 691, 674**
  - benefits 707, 708
  - identity 672-675
  - layers 692, 693
  - primitives 693, 694
  - properties 691
  - services 694
  - token, swapping 708, 709
  - Uniswap liquidity pool 710-714
  - Uniswap protocol 708
- decentralized finance (DeFi), services**
  - asset tokenization 694
  - Decentralized Exchanges (DEX) 695-697
  - derivatives 702, 703
  - flash loan 701, 702
  - insurance 704
  - lending and borrowing 704-707
  - money streaming 703
  - yield farming 703
- decentralized identifiers (DID) 665-670**
  - requirements 666
- decentralized identity and decentralized finance (DeFi) 49**
- decentralized identity model 657**
- decentralized marketplace 45**
- decentralized mesh network 740**
- decentralized NFT marketplace**
  - URL 739
- decentralized oracle 238**
- Decentralized Organizations (DOs) 42, 43**
- Decentralized Public Key Infrastructure (DPKI) 657**
- decentralized storage**
  - IPFS, using for deployment on 404-406
- decentralized system 31**
  - versus centralized system 33
- decentralized web 48**
- decrypted private key 253**
- decryption 52**
- decryption key 253**
- Deep Crack 74**
- DeFi attacks**
  - airdrop hunting 631
  - flash loan attacks 631
  - forged NFTs 631
  - identity spoofing 631
  - MEV/BEV 631
  - NFT DoS 631
  - sandwich attack 631
  - stable coins stability/security risks 631
  - unlimited (scarcity-free) token generation 631

- delegated PoS** 150
- demand-side economies of scale** 198
- Denial of Service (DoS) attack** 589, 623, 721
- deployment transactions** 458
- derivatives** 702
- derivative token** 476
- design principles, Hyperledger**
  - auditability 452
  - deterministic transactions 452
  - identity 451
  - interoperability 452
  - modular structure 451
  - portability 452
  - privacy and confidentiality 451
  - rich data queries 452
  - scalability 451
- deterministic wallets** 194
- development environment**
  - connecting, to test networks 305
  - private network, creating 305-307
  - setting up 304
- DeversiFi** 576
- DEVP2P wire protocol** 283, 290
- Diem protocol**
  - reference link 154
- Differential Power Analysis (DPA)** 636
- difficulty time bomb** 295
- Diffie-Hellman algorithms** 82
- diffusion** 591
- diffusion property** 71
- Digital Asset Holdings (DAH)** 444
- Digital Asset Modeling Language (DAML)** 243-245
  - reference link 244
- digital identity** 652
- digital identity, models**
  - centralized identity model 652, 653
  - decentralized identity model 657
  - federated identity model 653-657
  - self-sovereign identity 658
  - self-sovereign identity, components 659
- Digital Ledger Technology (DLT)** 23
- Digital Rights Management (DRM)** 20
- digital signatures** 73, 82, 98
  - aggregate signatures 108
  - blind signature 104
  - elliptic curve digital signature algorithm (ECDSA) 100, 101
  - multisignatures 105, 106
  - ring signatures 108, 109
  - RSA digital signature algorithms 98
  - threshold signatures 106, 107
  - types 104
- digital tree** 65
- digital wallet** 670, 671
  - governance frameworks 671, 672
  - verifiable data registries 671
- Digix gold tokens**
  - URL 475
- Directed Acyclic Graph (DAG)** 115, 312, 554, 602
- Directed Acyclic Graphs (DAGs)** 39
- Discovery protocol** 282
- discrete logarithm integrated encryption scheme (DLIES)** 83
- discrete logarithm problem, ECC** 93-95
- discrete logarithm scheme** 82
- DiscV4** 283
  - reference link 283
- DiscV5** 283
  - reference link 283
- disintermediation** 33
- Distributed Artificial Intelligence (DAI)** 740
- distributed consensus** 18
- Distributed Denial of Service (DDoS)** 290
- distributed hash table (DHT)** 66, 67

**Distributed Hash Tables (DHTs)** 9, 38

**distributed ledgers** 24, 444, 455

Besu 446

Fabric 444

Indy 446

Iroha 445

Sawtooth 445

**distributed system** 4-6, 30, 119

CAP theorem 6, 7

PACELC theorem 8

**Distributed Validator Protocol** 430

**Distributed Validator Technology (DVT)** 429

**distributive law** 80

**DLS protocol** 138

**documentation and coding guidelines, Solidity**

reference link 369

**Domain-Specific Languages (DSLs)** 229, 635

**domain-specific projects, Hyperledger** 448

Grid 448

**double and add algorithm** 92

**double-spending attack** 627

**DREAD model** 647

**Drizzle** 352

## E

**ECDSA digital signatures**

generating 102-104

**eclipse attack** 623, 624

**EIP-155** 626

**EIP155**

reference link 282

**EIP-1559** 296-298

**EIP-1559, variables**

baseFeePerGas 297

maxFeePerGas 298

maxPriorityFeePerGas 298

**electronic cash (e-cash)** 9, 10

accountability 9

anonymity 10

**Electronic Frontier Foundation (EFF)** 74

**Electrum**

URL 195

**elliptic curve** 83, 87

point addition 88-90

point doubling 88-92

point multiplication 92

**Elliptic Curve Cryptography (ECC)** 87, 159, 258

discrete logarithm problem 93-95

keys, generating with 95-97

mathematics 87, 88

**Elliptic-curve Diffie-Hellman (ECDH)** 83, 525

**Elliptic Curve Digital Signature Algorithm (ECDSA)** 83, 100, 160, 250, 638

using 101

**elliptic curve discrete logarithm problem (ECDLP)** 93

**Elliptic Curve Integrated Encryption Scheme (ECIES)** 83, 283

reference link 283

**elliptic curves algorithm** 83

**Embark** 352

**embedded consensus** 207

**enclave** 524, 587

**encoding schemes** 116

base58 117

base64 117

**encrypted private key** 253

**endorsing peers** 457

**enrolment certificate authority (E-CA)** 454

**enrolment certificates (E-Certs)** 454

**enterprise blockchain**

architecture 507

available platforms 515-517

- challenges 517
- versus public blockchain 506
- enterprise blockchain architecture**
  - application layer 509
  - governance layer 508
  - integration layer 508
  - network layer 507
  - privacy layer 508
  - protocol layer 508
  - security, performance, scalability, monitoring 509
- enterprise blockchain solutions**
  - business-oriented factors 499
  - designing 509
  - limiting factors 500, 501
- enterprise blockchain solutions, designing**
  - architecture development method (ADM) 511
  - Architecture development method (ADM) 512
  - cloud solutions 513, 514
  - TOGAF 510
- enterprise blockchains, requirements**
  - access governance 503
  - better tools 506
  - compliance 503, 504
  - consistency 501
  - ease of use 505
  - integration 505
  - integrity 501
  - interoperability 504
  - monitoring 505
  - performance 502, 503
  - privacy 502
  - secure off-chain computation 505
- Enterprise Blockonomics 518**
- enterprise dApps 503**
- Enterprise Ethereum Alliance (EEA) 3, 502**
- Enterprise Haskell 521**
- Enterprise Resource Planning (ERP) 499**
- enterprise solutions 498**
- enums 363**
- ephemeral keys 67**
- epidemic flooding 591**
- equity token offerings (ETOs) 477**
- ERC-20 interface**
  - functions and events 483-485
- ERC-20 token**
  - adding, in MetaMask 493-495
  - building 483
  - contract, deploying on Remix JavaScript virtual machine 488-493
  - Solidity contract, building 483-488
- ERC-20 token standard 480**
  - reference link 480
- ERC-223 token standard 480**
- ERC-721 token standard 480**
- ERC-777 token standard 480**
- ERC-884 token standard 480**
- ERC-1155 token standard 482**
  - reference link 482
- ERC-1400 token standard 481**
  - ERC-1066 481
  - ERC-1410 481
  - ERC-1594 481
  - ERC-1643 481
  - ERC-1644 481
- ERC-1404 token standard 481**
  - reference link 481
- ERC-4626 token standard 482, 483**
  - reference link 482
- error handling constructs, Solidity**
  - assert 368
  - require 368
  - revert 368
  - throw 368
  - Try/Catch 368
- Eth capability protocol**
  - reference link 284

**ether** 250, 729

**Ethereum** 407, 522, 598, 625

future roadmap 440

identity 672

innovations 295

reference link 622

staking on 412-415

transactions 294

**Ethereum, after The Merge** 408, 409

Beacon Chain 409, 410

dimensions 408, 409

P2P interface (networking) 421, 422

**Ethereum block**

difficulty mechanism 278

finalization 277

processing 277, 278

validation 276, 277

**Ethereum blockchain** 247, 248

ecosystem architecture 249

interacting, with MetaMask 321

programming languages 287, 344

state transition function 267

**Ethereum blockchain, elements** 249

accounts 254

cryptocurrency 250

Ethereum network 281

EVM 270-272

keys and addresses 250-254

messages 265, 266

miners 279

nodes 279

precompiled smart contracts 286, 287

transactions 255

wallets 289

**Ethereum blocks**

elements 274

**Ethereum Classic (ETC)** 250, 625

**Ethereum environment (EOAs)** 265

**Ethereum Go client**

URL 305

**Ethereum Homestead** 264

**Ethereum improvement proposals (EIPs)** 295, 432

reference link 480

URL 295

**Ethereum, innovations**

difficulty time bomb 295

EIP-1559 296-298

merge and upgrades 298

**Ethereum Name Service (ENS)** 508

**Ethereum network** 281

DEVP2P 283

Discovery protocol 282, 283

main net 282

private nets 282

RLPx 283

sub-protocols 283

test nets 282

**Ethereum Virtual Machine (EVM)** 241, 247, 270-272, 278, 344, 411

execution environment 273

machine state 273, 274

**Ethereum WebAssembly (ewasm)** 272

reference link 272

**Ethereum yellow paper**

reference link 248

**Ethlance** 44

URL 45

**European Union Agency for Network and Information Security (ENISA)** 744

**events, Solidity** 366

**EVM networks**

reference link 272

**EVMs (ZK-EVMs)** 569

**execution client** 411, 423

**execution layer** 298

**extendable-output functions (XOFs)** 61

**extended protocols, Bitcoin** 206

- colored coins 206, 207
- counterparty 207, 208

**external function calls** 357

**external functions** 356

**externally owned account (EOA)** 254, 265

- properties 254, 255

**External Owned Accounts (EOAs)** 693

## F

**Fabric** 444, 452, 515

- core capabilities 453
- messages 456
- reference link 444

**Fabric 2.0** 465

- new chaincode application patterns 466, 467
- new chaincode lifecycle management 465, 466
- reference link 465

**Fabric, applications** 459

- application model 462
- chaincode implementation 460, 461

**Fabric, components**

- channels 457
- clients 457
- crypto service provider 459
- membership service provider 458
- nodes 457
- peers 457
- private data collections (PDCs) 458
- smart contracts 459
- transactions 458
- world state database 457, 458

**Fabric, consensus mechanism**

- ordering 462
- transaction endorsement 462
- validation and commitment 462

**Fabric, key concepts** 452, 453

- APIs and CLIs 456
- blockchain services 454
- membership service 453, 454
- smart contract services 456

**Fabric, transaction flow**

- steps 463, 464

**failure detectors** 121

**fallback functions** 358

**faster consensus mechanisms** 555

**Fast Reed-Solomon IOP of Proximity (FRI)** 597

**fault tolerance** 120

**fault-tolerant algorithms**

- Byzantine fault-tolerance (BFT) 120
- crash fault-tolerance (CFT) 120

**Federal Information Security Management Act (FISMA)** 517

**federated identity model** 653-657

**Feistel cipher** 71

**Fiat-Shamir (FS)** 609

**field**

- cardinality 80
- finite field 80
- order 80
- prime field 80

**Field Programmable Gate Arrays (FPGAs)** 185, 742

**Filament** 721

**Filecoin** 39

**Financial Conduct Authority (FCA)** 504, 743

**financial instruments**

- attributes 683

**financial markets** 681

- exchanges 682
- trading 681



**financial markets, exchanges**

- order management and routing systems 683
- orders and order properties 682, 683
- trade, components 683
- trade lifecycle 684, 685

**finite field 80****firewalls 732****flash loan 701, 702****flash loan attack 631****FLP impossibility result 121****Fluff phase 591****FoldingCoin 739**

- URL 739

**foreign exchange (forex) 474****forged NFTs 631****forking 627****forks 179, 281**

- hard fork 180
- soft fork 180
- temporary forks 180
- types 180

**formal specifications 639****formal verification 639, 644**

- model checking 641-643
- of smart contracts 640, 641

**Frama-C**

- URL 644

**frontend attacks**

- account hacking 633
- DoS attacks 633
- malicious scripts 633
- misaligned frontend 633

**frontend webpage**

- creating 387-391

**Frontier 281****Fuel v1 576****full-ecosystem decentralization 38**

- communication 39, 40
- power, computing 40-42
- storage 38, 39

**fully private blockchain 25****function modifiers, Solidity**

- override 359
- payable 358
- pure 358
- view 358
- virtual 359

**functions, Solidity 355**

- constructor functions 358
- external function calls 357
- external functions 356
- fallback functions 358
- function modifiers 358
- function signature 356
- function visibility specifiers 358
- input parameters 356
- internal function calls 357
- internal functions 356
- modifier functions 358
- output parameters 357
- syntax 356

**function visibility specifiers, Solidity**

- external 358
- internal 358
- private 358
- public 358

**fungible tokens 473**

- divisible, working principle 473
- indistinguishable, working principle 473
- interchangeable, working principle 473
- working principle 473

**G****Galois counter (GCM) mode 74****Galois fields 80**

**Ganache** 348  
**ganache-cli** 348  
**ganache-ui** 349-351  
**gas** 262, 263  
**gas limit field** 258  
**Gasper PoS** 410  
**gas price field** 258  
**Gemini Dollar (GUSD)**  
     URL 475  
**General-Purpose I/O (GPIO) pins** 722  
**general-purpose programming languages (GPLs)** 230  
**genesis block** 178, 276  
**genesis file** 15, 285  
     parameters 285  
**genesis transaction** 227  
**Geth**  
     account, creating 299-301  
     POST requests, used for interacting with 380, 381  
     used, for interacting with contracts 371, 372  
     used, for querying blockchain 301  
     used, for querying contracts 377-380  
**Geth attach** 301, 302  
**Geth client** 248, 289  
     configuring 299  
     installing 299  
**Geth console** 301  
**Geth JavaScript console**  
     experimenting with 310, 311  
**Geth JSON RPC** 301-304  
**Geth RPC APIs**  
     reference link 304  
**global stabilization time (GST)** 123  
**global variables** 359, 360  
**Gluon** 576

**Goerli test network** 322  
**Golem** 45  
     URL 45  
**Google RPC (gRPC)** 455  
**GoQuorum plugins**  
     reference link 542  
**governance frameworks** 671, 672  
**government functions, blockchain**  
     border control 735-737  
     citizen identification 737, 738  
     elections 737  
**GPU** 184  
**Greediest Heaviest Observed SubTree (GHOST)** 279, 421, 553  
**GreenAddress** 195  
**Grid** 444, 448  
     reference link 448  
**group signatures** 593

## H

**Hadamard Product Relation (HPR)** 602  
**handshaking** 283  
**hard fork** 180  
**hardware description languages (HDLs)** 185  
**hardware device-assisted proofs** 234  
     Android proof 234  
     Ledger proof 234  
     trusted hardware-assisted proofs 235, 236  
**hardware layer, blockchain** 622, 623  
**hardware oracles** 236  
**Hardware Security Module (HSM)** 194, 637  
**Hardware Security Modules (HSMs)** 451, 505  
**hardware wallets** 195  
**hash-based commitment schemes** 596  
**hash-based MACs (HMACs)** 69  
**hash collision attack** 240

**hash functions 56, 57**

- applications 63
- message digest (MD) functions 57
- messages, encrypting with SHA-256 62, 63
- properties 56
- secure hash algorithms (SHAs) 57, 58
- security properties 56

**hash pointer 19****hexadecimal literals 363****hierarchical deterministic wallets 194, 195****High-Performance Computing (HPC) 505****Homestead 281, 348****homomorphic encryption 109, 587, 741**

- fully homomorphic system 109
- partially homomorphic system 109

**Horn solving 641****HotStuff 151, 152**

- chain quality 151
- commit phase 153
- decide phase 153
- linear view change 151
- liveness 154
- optimistic responsiveness 151
- pre-commit phase 153
- prepare phase 153
- safety 154

**HTTP REST interface**

- using 218, 219

**hybrid encryption schemes 83****Hyperledger**

- APIs and SDKs 450
- communication 450
- consensus 450
- data store 450
- design principles 451, 452
- policy services 450
- projects 444
- reference architecture 449, 450

- security and crypto 450
- smart contracts 450
- URL 444

**Hyperledger Fabric blockchain**

- capabilities 453

**Hyperledger Indy 675****Hyperledger Landscape**

- URL 444

**Hyperledger project 515****Hyperledger Ursa 675****I****IBD node 190****IBFT 531**

- Quorum network, setting up with 532

**IBM 444**

- reference link 514

**identity 651, 652**

- in DeFi 672-675
- in Ethereum 672
- in Metaverse 672-675
- in Web3 672
- in world of Web3 673-675

**Identity and Access Management Systems (IAMs) 655**

- challenges 656

**identity mixer 454****Identity Provider (IDP) 655****identity spoofing 631****iExec**

- URL 239

**Immutable X 576****impersonation attack 635****inbound connections 421****inbound oracles 236**

- inbound oracles, types**
  - aggregation based oracles 237
  - computation oracles 237
  - crowd wisdom-driven oracles 237, 238
  - decentralized oracle 238
  - hardware oracles 236
  - smart oracles 238
  - software oracles 236
- indistinguishable obfuscation (IO)** 586, 587
- Indy** 444, 446
  - reference link 446
- Infrastructure as a Service (IaaS)** 513
- Infura**
  - URL 321
- inheritance, Solidity** 367
- Initial Block Download (IBD) node** 189
- Initial Coin Offering (ICO)** 476, 716
- initial currency offering (ICO)** 476, 477
- initial exchange offering (IEO)** 477
- initialization vector (IV)** 68, 253
- initial public offerings (IPOs)** 476, 477
- inner padding (ipad)** 69
- insecure key storage** 637
- Institute of electrical and electronics engineers (IEEE)** 3
- integer factorization schemes** 82
- integer literals** 363
- integer overflow and underflow** 628, 629
- integers** 361, 362
- Integrated Development Environments (IDEs)** 318
- integrated encryption scheme (IES)** 83
  - discrete logarithm integrated encryption scheme (DLIES) 83
  - elliptic curve integrated encryption scheme (ECIES) 83
- IntelliSense** 353
- Intel Software Guard Extensions (Intel SGX)** 445
- Interactive Oracle Proof (IOP)** 597, 605
  - classes, categorizing 605
- interface layer, blockchain**
  - attacks on wallets 632, 633
  - oracle attacks/oracle manipulation attacks 632
- internal function calls** 357
- internal functions** 356
- International Civil Aviation Organization (ICAO)** 735
- international standards organization (ISO)** 3
- Internet of Things (IoT)** 231, 716
- Internet Service Providers (ISPs)** 39
- interoperability** 504
- Inter-Planetary File System (IPFS)** 39, 49
  - IRL 49
- Inter-Process Communication (IPC)** 309
- Invertible Bloom Lookup Tables (IBLTs)** 553
- Invisible Internet Project (I2P)** 586
- invocation transactions** 458
- IoT, and blockchain convergence**
  - benefits 719-721
- IoT architecture** 716, 717
  - application layer 718, 719
  - device layer 718
  - management layer 718
  - network layer 718
  - physical object layer 718
- IPFS** 352, 736
  - used, for deployment on decentralized storage 404-406
- IPv6** 719
- Iroha** 444, 445
  - reference link 445
- Isabelle**
  - URL 640
- Istanbul** 348

**Istanbul Byzantine Fault Tolerance (IBFT)** 119, 120, 134-137, 430  
consensus states 136  
references 137  
versus Practical Byzantine Fault Tolerance (PBFT) 134, 135  
working 135

## J

**JavaScript Object Notation (JSON)** 302  
**JavaScript runtime environment (JSRE)** 398  
**Jaxx**  
URL 195  
**JSON RPC**  
URL 302  
**JSON RPC interface**  
using 217, 218  
**JSON Web Signature (JWS)** 664  
**Just a Bunch of Key wallets** 194

## K

**Kadcast** 551  
**Keccak** 61  
**key derivation function (KDF)** 68, 252, 253  
**keyed hash functions** 68  
**key escrow attack** 637  
**key establishment mechanisms** 82  
**keyless primitives** 55  
hash functions 56, 57  
random numbers 55  
**key loss or theft** 637  
**key management-related vulnerabilities and attacks**  
insecure key storage 637  
key escrow attack 637  
key loss or theft 637  
unauthorized key sharing 637

**key reuse attack** 636  
**keys**  
generating, with ECC 95-97  
**keystream** 72  
**key stretching** 195  
**Know Your Customer (KYC)** 197, 503

## L

**languages, Ethereum blockchain**  
Low-level Lisp-like Language (LLL) 344  
Mutan 344  
Serpent 344  
Solidity 344  
Vyper 344  
Yul 344  
**Last in, First Out (LIFO)** 170, 270  
**Latest Message Driven Greediest Heaviest Observed SubTree (LMD GHOST)** 419, 421, 438  
**layer 1 blockchain** 26  
monolithic blockchain 26  
polylithic blockchain 26  
**layer 2 blockchain** 26  
sidechains 26  
**Layer2 Finance** 576  
**LED** 722  
**Ledger Blue** 234  
**ledger decoupling** 445  
**Ledger Nano S** 234  
**Ledger proof** 234  
**ledger storage** 456  
**Legal Knowledge Interchange Format (LKIF)** 225  
**length extension attack** 636  
**Libbitcoin**  
URL 219

**Libra**

URL 475

**libraries, Hyperledger project 446**

Anonymous Credentials (AnonCreds) 447

Aries 446

Transact 447

Ursa 447

**libraries, Solidity 367****LibUrsa 447****LibZmix 447****light clients 289****Light Emitting Diode (LED) 722****Light Ethereum Sub-protocol (LES) 283****Lightweight Directory Access Protocol (LDAP) 454****Linear Temporal Logic (LTL) 642****literals 363**

enums 363

hexadecimal literals 363

integer literals 363

string literals 363

**loan mechanism**

actors 704, 705

**local variables 359****log replication 129****log series 266****London 348****Loopring 576****lower bound result 122****Low-level Lisp-like Language (LLL) 287, 344****low watermark 133****M****mac 253****machine learning 740****Machine-Readable Travel Document (MRTD) 735****Machine-Readable Zone (MRZ) 735****main net 282****Man-in-the-Middle (MITM) attack 635****Manticore**

reference link 645

**mappings 364****MasterCoin 716****master key 67****mathematical concepts 79**

field 80

group 80

modular arithmetic 79

sets 80

**mathematical puzzle 181****Mauve Paper**

reference link 554

**Maximal Extractable Value (MEV) 434****maximum achievable decentralization (MAD) 35****maximum value 237****mean value 237****median value 237****membership service, Fabric 453, 454****membership service provider (MSP) 453, 458****memory-bound PoW 146****memory hard computational puzzles 147****memory pool (mempool) 205****merged fee market 435****Merkelized Alternative Script Tree (MAST) 206****Merkle-Damgard construction 57****Merkle Patricia Tree (MPT) 65, 66, 256, 257, 572**  
nodes, types 65**Merkle Patricia trie (MPT) 523****Merkle root 15, 64, 256**

ReceiptsRoot 257

StateRoot 257

TransactionsRoot 257

- Merkle trees** 64, 65, 256
- mesh communication topology** 152
- mesh network** 740
- message authentication** 53
- message authentication codes (MACs)** 53, 68
  - hash-based message authentication codes 69
- message call transactions** 258, 265
- message digest (MD) functions** 57
- message passing** 119
- messages** 265
  - components 265, 266
- messages, Fabric**
  - consensus messages 456
  - discovery messages 456
  - synchronization messages 456
  - transaction messages 456
- messages, PBFT** 132
- messages, Tendermint** 143
  - pre-commit 142
  - pre-vote 142
  - proposal 142
- MetaMask** 483
  - accounts, importing with keystore files 328-331
  - custom network, adding 325-327
  - custom network, adding to connect with Remix IDE 325-327
  - installing 321, 322
  - Remix IDE, used for interacting contract through 336-342
  - used, for creating account 322-324
  - used, for deploying contract 331-335
  - used, for funding account 322-324
  - used, for interacting with Ethereum Blockchain 321
  - using, to deploy smart contract 324
- MetaMask wallet** 289
- Metaverse**
  - identity 672-675
- metaverses** 49
- Metis Andromeda** 576
- MEV/BEV** 631
- MimbleWimble** 592
- Miner Extractable Value (MEV)** 436, 700
- miner node**
  - functions 279
- minikey** 159
- minimum feasible decentralization (MFD)** 35
- mining** 19
- mining algorithm**
  - steps 182
- mining pool** 186
- mining systems** 184
- mini private key format** 159
- Miniscript** 175
  - reference link 175
- mixing protocol** 588, 589
- mnemonic code** 194
- mobile wallets** 195
- model checking** 641-643
- modifier functions** 358
- modulus** 79
- Monero** 109, 110
- money streaming** 703
- MPC-based approach** 600
- Multichain blockchains**
  - reference link 106
- multichain solutions** 549
- multiparty computation (MPC)** 600
- multi-party non-repudiation (MPNR) protocols** 54
- Multi-Signature (M of N)** 431
- multisignatures** 105, 106
- MultiSig (Pay to MultiSig)** 172

**Musicoïn**

URL 739

**Mutan 344****MVC-B architecture 462**

blockchain logic 462

control logic 462

data model 462

view logic 462

**N****Nakamoto coefficient 35**

reference link 35

**Nakamoto consensus 120, 144**

properties 146

versus traditional consensus 145

**Namecoin 42, 715**

reference link 715

**National Institute of Standards and Technology (NIST) 57****native contracts 286****Near Field Communication (NFC) 195, 588****network effect 198****network ID 284****networking functions 428****network layer, blockchain**

DoS attack 623

eclipse attack 623, 624

network spoofing 624

Sybil attack 623

**network model 138****network spoofing 624****new chaincode application patterns, Fabric 2.0 466, 467****new chaincode lifecycle management, Fabric 2.0 465, 466****New Out Of Box Software (NOOBS) 723**

download link 723

**New York Stock Exchange (NYSE) 682****NFT DoS 631****node 4****Node.js 347**

installation link 532

URL 347

**nodes, Fabric**

orderer nodes 457

**node types, Merkle Patricia tree**

branch nodes 65

extension nodes 65

leaf nodes 65

null nodes 65

**nonce 15, 68, 258****non-deterministic wallets 194****Non-Fungible Tokens (NFTs) 2, 473, 706**

indivisible 474

non-interchangeable 474

unique 474

**non-outsourceable puzzles 151****not colored coins 207****nothing at stake problem 150, 627****Null data/OP\_RETURN 172****Nxt**

URL 150

**O****off-chain solutions 546, 555, 556****OMG Network 576****Ommers validation 277****OMNI network**

URL 45

**on-chain scaling solutions 551****on-chain solutions 546****one-way pegged sidechain 26****Onion Router 586****online wallets 195**



**opcodes** 170, 171, 288

reference link 289

**Open Authorization (OAuth)** 654

**OpenBazaar**

URL 228

**Openchain**

reference link 106

**OpenID** 655

**open phase** 110

**Open Web Application Security Project (OWASP)** 647

**OpenZeppelin toolkit** 353

reference link 353

**OpenZeppelin** 495

reference link 495

**optimal decentralization point (ODP)** 35

**optimistic rollups** 563, 564, 575

advantages 564

disadvantages 564

vs ZK-rollups 573

**Oracle** 685

reference link 514

**oracle-as-a-service platforms** 239

**oracle attacks**

bribing oracles 632

Denial of Service (DoS) attack 632

freeloading attacks 632

oracle censorship 632

Sybil attacks 632

tampering with data sources 632

**oracle, is Truebit**

URL 237

**oracle manipulation attack** 629, 630

preventing 630

**oracles** 121, 231-233

standard mechanics 232

use cases 231

**order book-based DEX** 698

**orderer** 454

**orderer nodes** 457

**orphan block** 179

**Ouroboros PoS consensus mechanism, Cardano**

URL 150

**outbound connections** 421

**outbound oracle** 238

**outer padding (opad)** 69

**Out of Gas (OOG)** 264

**output feedback (OFB) mode** 74

**Over-the-Counter (OTC)** 681

**Oyente** 644, 645

URL 645

## P

**P2P interface (networking)** 421, 422

elements 421

**P2P networks** 736

**PACELC theorem** 8

**Pacemaker** 151, 154

**Pact** 742

**PageSigner project**

reference link 233

**paper wallets** 195

**parallel computing** 31

**partially homomorphic encryptions (PHEs)** 109

**passive replication** 120

**Password-Based Key Derivation Function 1 (PBKDF1)** 68

**Paxos (PAX)** 123-125

URL 475

working 126, 127

**Pay2Taproot (P2TR)** 206

**payment channels** 556

**Pay-to-Public-Key Hash (P2PKH)** 172

**Pay-to-Script Hash (P2SH)** 172

- PBFT, in Hyperledger Sawtooth**
  - reference link 134
- Pedersen commitments** 592, 596
- Pedersen commitment scheme** 111
  - reference link 111
- Peercoin**
  - URL 150
- peers, Fabric**
  - committing peers 457
  - endorsing peers 457
- Peer-to-Peer (P2P)** 186, 446, 507, 689, 719
  - protocol 455
- pegged sidechains** 26, 209
- Peggy character** 111
- permissioned ledger** 25
- Personal Package Archives (PPAs)** 344
- Petersburg** 348
- physical unclonable functions** 742
- Plasma** 558, 575
  - URL 559
  - vs Sidechains 559
- Platform as a Service (PaaS)** 721
- point addition** 88, 89
  - example 89, 90
- point doubling** 91
  - example 92
- point multiplication** 92
- Point of Sale (POS) terminals** 200
- policies** 454
- Polkadot** 549-551
- Polkadot BABE** 118
- Polygon** 576
  - scalability solutions 576, 577
- Polygon Po** 577-579
- polynomial commitment scheme (PCS)** 605
  - categories 606
- polynomial commitment schemes** 596
- Polynomial Interactive Oracle Proof (PIOP)** 605, 606
- post-quantum cryptography** 638
- POST requests**
  - used, for interacting with Geth 380, 381
- post-trade settlement** 685
- PoW, alternatives** 147, 148
  - non-outsourceable puzzles 151
  - Proof of Activity (PoA) 150
  - Proof of stake (PoS) 148-150
  - Proof of Storage 148
- Practical Algorithm to Retrieve Information Coded in Alphanumeric (PATRICIA)** 65
- Practical Byzantine Fault Tolerance (PBFT)** 119, 120, 123, 129, 131, 643
  - certificates 131
  - checkpointing protocol 133
  - checkpointing subprotocol 129
  - commit phase 130
  - Istanbul Byzantine Fault Tolerance (IBFT) 135
  - limitations 134
  - messages 132
  - normal operation subprotocol 129
  - prepare phase 130
  - pre-prepare phase 129
  - strengths 134
  - versus Istanbul Byzantine Fault Tolerance (IBFT) 134
  - view change protocol 132, 133
  - view change subprotocol 129
  - working 130
- precompiled contracts** 286, 287
- preimage attack** 636
- preimage resistance** 56
- prime field** 80
- privacy**
  - anonymity 502
  - confidentiality 502

- private blockchains** 24, 553
- private data collections (PDCs), Fabric** 458
- private graph construction phase** 591
- private key** 67, 80, 159, 160, 250-252
- private net** 282
  - components, requisites 284, 285
- private network**
  - creating 305-307
  - Geth JavaScript console, experimenting with 310, 311
  - initializing 307-310
  - transactions, mining 312-318
  - transactions, sending 312-318
- private transaction manager** 525
- Proactive Market Maker (PMM) model** 700
- Probabilistic Polynomial Time (PPT)** 596
- Program Counter (PC)** 273
- programming languages, Ethereum blockchain**
  - opcodes 288, 289
  - runtime bytecode 288
  - Solidity 287, 288
- projects, Hyperledger** 444
  - distributed ledgers 444
  - domain-specific 448
  - libraries 446
  - tools 447
- Proof of Activity (PoA)** 150
- proof of authenticity** 233
- Proof of Authority (PoA)** 523
- Proof of Burn (PoB)** 148, 209
- proof of coinage** 148
- Proof of Concept (PoC)** 498
- Proof of Deposit** 148
- Proof of Elapsed Time (PoET)** 445, 742
- proof of ownership** 209
- proof of retrievability** 148
- proof of stake (PoS)** 26, 46, 119, 148-150, 295, 409, 503, 553, 626
- proof-of-stake (PoS)** 415-421, 430
- Proof of Storage** 148
- proof of validity** 233
- Proof of Work (PoW)** 7, 46, 63, 119, 144, 165, 181, 182, 183, 184, 204, 295, 500
  - CPU-bound PoW 146
  - memory-bound PoW 146
  - working 145
- Proofs of Knowledge (PoK)** 447
- Propose Builder Separation (PBS)** 435, 437
- proprietary blockchain** 25
- protocol messages**
  - types 187
- provable**
  - URL 239
- pseudorandom number generators (PRNGs)** 55
- public blockchain** 24
  - versus enterprise blockchain 506
- public key** 81, 251
- public key cryptography** 10, 80-82, 635
  - brute-force attack 635
  - impersonation attack 635
  - key reuse attack 636
  - Man-in-the-Middle (MITM) attack 635
  - side-channel attack 636
- Public Key Infrastructure (PKI)** 108, 131, 451, 657, 736
- public keys** 67, 160
  - identifying, by prefixes 160
- public-key schemes** 83
- puzzle-promise** 590
- Pycoin**
  - URL 219

## Q

**quadratic arithmetic program (QAP)** 115

**quantum key distribution (QKD)** 638

**quantum-safe signature schemes** 638

**Quorum** 515, 522

access control, with permissioning 529, 530, 531

architecture 522

cryptography 525

performance 531

pluggable architecture 542, 543

pluggable consensus 531

privacy 525-527

projects 542, 543

reference link 543

**Quorum network, setting up with IBFT** 532

Geth, attaching to nodes 535-537

investigating, with Geth 539-542

private transaction, running 535

Quorum Wizard, installing 532-535

transaction, viewing in Cakeshop 538

**Quorum, on Azure**

reference link 543

**Quorum, on Kaleido**

reference link 543

**Quorum privacy**

enclave decryption 528, 529

enclave encryption 527

transaction propagation 527

**Quorum Wizard**

installing 532-535

## R

**RACE Integrity Primitives Evaluation Message Digest (RIPEMD)** 58

**Radio-Frequency Identification (RFID) tags** 718

**Radix tree** 65

**Raft** 467, 531

**Raft protocol** 127-129

subproblems 127

**Raiden** 557

**RANDAO** 426

**randomized algorithms** 122

**random line of nodes** 591

**random number generators (RNGs)** 55

**random numbers** 55

random strings, generating 55, 56

**range proof** 585

**Rank 1 Constraint System (R1CS)** 115

**Raspberry Pi** 722

URL 722

**Raspbian**

installation link 723

**Realitio project**

URL 239

**real randomness** 55

**Recursive Length Prefix (RLP)** 261

reference link 261

**Redundant Byzantine Fault Tolerance (RBFT)** 446

**Reed-Solomon error correction**

using 159

**reentrancy bug** 241, 629

**reference architecture, Hyperledger** 449, 450

**reference types** 361, 363

arrays 363

mappings 364

structs 363, 364

**refund balance** 267

**regulatory compliance** 649

**Relying Parties (RPs)** 655

**Remix IDE** 318-321, 483, 729

custom network, connecting with 325-327

URL 483

used, for interacting contract through  
MetaMask 336-342

using, to deploy smart contract 324

### **Remix plugin**

reference link 542

**Remote Procedure Calls (RPCs)** 190, 248

**replay attack** 625

**replicated state machine (RSM)** 127, 521

### **replication** 120

active replication 120

passive replication 120

state machine replication (SMR) 120

**resistor** 722

**restricted private transactions** 502

**return on investment (ROI)** 476

**reverse oracle** 238

**reward application** 277

**ribbon cable connector** 722

### **Ricardian contract, objects**

code 228

parameters 228

prose 228

**Ricardian contracts** 225-229

properties 225

**ring signatures** 108, 109, 593

**Ripple labs (codius)** 238

**RLPx** 283

reference link 283

**Role-Based Access Control (RBAC)** 503

reference link 530

### **rollups** 559, 560

data availability 560, 561

data validity 560

optimistic rollups 563, 564

types 563

working with 561, 562

**Ropsten** 354

**round functions** 71

### **RSA** 83

decrypting with 85-87

encrypting with 85-87

key generation process 83

**RSA digital signatures** 98

authenticity 99

generating 100

non-reusability property 99

operation 99

unforgeability property 99

**RSA puzzle solver** 590

**runtime bytecode** 288

## **S**

**Sabre** 447

### **safe curves**

reference link 95

### **SAFE Network**

reference link 45

### **SafetyNet**

reference link 234

**salt** 68

**sandwich attack** 631

**Sawtooth** 444, 445, 515

reference link 445

**S-boxes** 71

**scalability** 545, 546

blockchain trilemma 546-548

categories 549

improving, methods 548

multichain solutions 549

off-chain solutions 555, 556

on-chain scaling solutions 551

Polkadot 549-551

rollup solutions 559, 560

**scalability, off-chain solutions**

- commit chains 559
- Plasma 558
- Plasma chains, versus sidechains 559
- sidechains 557
- state channels 556, 557
- sub-chains 557
- tree chains 558
- trusted hardware-assisted scalability 559

**scalability, on-chain scaling solutions**

- Bitcoin-NG 554
- block interval reduction 553
- block propagation 553, 554
- block size, increasing 552
- bloXroute 551
- DAG-based chains 554
- faster consensus mechanisms 555
- Invertible Bloom Lookup Tables 553
- kadcast 551
- private blockchains 553
- sharding 553
- transaction parallelization 552

**scalability, rollup solutions**

- data availability 560, 561
- data validity 560
- example 577
- fraud proof-based classification 575-577
- multilayer solutions 579, 580
- optimistic rollups 563, 564
- optimistic rollups, versus ZK-rollups 573
- Polygon PoS 577-579
- types 563
- usage 561, 562
- validity proof-based classification 575-577
- ZK-EVM 570-573
- ZK-Rollups 564-566
- ZK-Rollups, building technologies 566-569
- ZK-ZK-rollups 573

**scalability trilemma 440****scalar point multiplication 92****Schnorr signatures 205****Script 16, 170, 222****Script 68****second pre-image resistance 56****secret key ciphers 69**

- block ciphers 71
- stream ciphers 70

**secret key cryptography 67****secret key (KEY) 73****secret prefix 69****secret sharing scheme 109****secret suffix 69****secure element (SE) 195****secure hash algorithms (SHAs) 57, 58**

- RIPEMD 58
- SHA-0 57
- SHA-1 58
- SHA-2 58
- SHA-3 58
- SHA-3 (Keccak) 61, 62
- SHA-256 58-60
- Whirlpool 58

**secure multiparty computation (SMPC) 502, 587****security analysis tools and mechanism 638, 639**

- formal verification 639, 640
- smart contract security 644, 645

**Security Assertion Markup Language (SAML) 654****security, blockchain 619-621****security protocol 54****security token offerings (STOs) 476, 477****seed 55****Segregated Witness (SegWit) 164, 202, 552**

- improvements 202, 203
- transactions 203, 204

**selective disclosure 584**

- self-destruct set** 266
- selfish mining attack** 627
- Self-Sovereign Identity (SSI)** 658
  - components 659
  - decentralized identifiers 665-670
  - digital wallet 670, 671
  - verifiable credentials 659
- semi-private blockchains** 24
- send fail issue** 628
- separation of concerns** 528
- Sepolia**
  - URL 489
- Sepolia test net**
  - reference link 305
- serialization** 261
- Serpent** 344
- Seth** 447
- SHA3-256 hash function** 253
- SHA-3 (Keccak)** 61, 62
- SHA-256** 58-60
  - hash computation 59
  - messages, encrypting with 62
  - pre-processing 58
- Shapella** 440
- sharding** 432-440, 553
- shared key cryptography** 67
- shared ledger** 24
- shared memory** 119
- sidechains** 26, 557
- side-channel attack** 636
- Silk Road marketplace** 593
- Simple Payment Verification (SPV)**
  - clients 289
  - nodes 192
- Simple Serialize (SSZ)** 422
- simple transaction** 258, 264
- simulator** 603
- Single Board Computer (SBC)** 722
- single-factor authentication** 53
- Single Sign On (SSO)** 508, 654
- slashing** 413
- Slither** 645
- smart contract engines** 447
- smart contract, oracles**
  - hardware device-assisted proofs 234
  - software and network-assisted proofs 233
- smart contracts** 37, 42, 174, 221, 222
  - deploying 240, 241, 354
  - deploying, with MetaMask 324
  - deploying, with Remix IDE 324
  - oracles 231-233
  - properties 222-224
  - real-world application 224, 225
  - technology 242
  - testing 353
  - Truffle, used for testing and deploying 399-404
  - writing 353
- smart contract security** 644
- smart contract services, Fabric** 456
  - events 456
  - secure container 456
  - secure registry 456
- smart contract, technology**
  - Digital Asset Modeling Language 243-245
  - Solana Sealevel 242
- smart contract templates** 229, 230
- smart contract vulnerabilities** 628
  - integer underflow and overflow 629
  - oracle manipulation attack 629, 630
  - reentrancy 629
  - send fail issue 628
  - timestamp dependency bugs 628
  - unguarded selfdestruct 629
  - unprivileged write to storage 629

- smart oracles** 238
- SMR problem** 9
- SMT (Satisfiability Modulo Theories)** 641
- SNARKs**
  - types 601
- soft fork** 180
- software and network-assisted proofs** 233
  - TLS-N-based mechanism 233
  - TLSNotary 233
- Software Guard Extensions (SGX)** 587, 742
- software oracles** 236
- Solana Sealevel**
  - reference link 242
- solc** 287
  - experimenting with 345-347
  - installing 344, 345
  - used, for generating ABI and code 376, 377
- Solgraph** 646
  - URL 646
- Solidity** 287, 344, 354, 628, 736, 742
  - control structures 365, 366
  - data types 361
  - error handling 368
  - events 366
  - features 354, 355
  - functions 355-359
  - inheritance 367
  - libraries 367
  - reference link 288
  - variables 359
- Solidity compiler** 344
- Solidity language** 529
- speed** 502
- sponge and squeeze construction** 61
- spreading phase** 591
- SSI-specific blockchain projects** 675
  - AnonCreds 675
  - Aries 675
  - challenges 676, 677
  - Hyperledger Indy 675
  - initiatives 676
  - other projects 676
  - Ursa 675
- SSI stack**
  - four-layer model 671
- SSL stripping** 635
- stable coins stability** 631
- stable tokens** 474
  - algorithmically stable 475
  - commodity collateralized 475
  - crypto collateralized 475
  - fiat collateralized 475
- stake grinding attack** 627
- stale block** 179
- standard transaction scripts** 171
- state and nonce validation** 277
- state channels** 556
  - performing, steps 556
- state machine replication (SMR)** 6, 120
- states, Ethereum blockchain**
  - account state 268
  - world state 268
- state variables** 360
- state variables, modifiers**
  - constant 361
  - immutable 361
- state variables, Tendermint** 143
  - lockedRound 143
  - lockedValue 143
  - step 143
  - validRound 143
  - validValue 143
- state variables, visibility scope**
  - internal 360
  - private 360
  - public 360



**static keys** 67

**status** 49

- reference link 49

**Steemit** 49

- URL 49

**Stem phase** 591

**storage root** 268

**stream ciphers** 69, 71

- operation 70
- types 70

**STRIDE model** 647

- benefits 647
- implementing 648

**string literals** 363

**structs** 363, 364

**structured reference string (SRS)** 601

**sub-chains** 557

- reference link 557

**subnets** 417

**substitution-permutation network (SPN)** 71

**subverted approach** 600

**Succinct Non-Interactive Argument of Knowledge** 598

**suicide set** 266

**Swarm** 283, 290, 291, 352, 736

- reference link 291

**Sybil attack** 144, 623

**symbolic execution** 645

**symmetric cryptography** 51, 67, 68

**symmetric-key schemes** 83

**synchronization modes**

- full 299
- light 299
- snap 299

**synchrony assumptions** 122

**sync node** 189

**system model, Tendermint**

- network model 138
- processes 138
- security and cryptography 139
- state machine replication 139
- timing assumptions 139

## T

**Taproot** 205

- Merkelized Alternative Script Tree (MAST) 206
- Pay2Taproot (P2TR) 206
- Schnorr signatures 205

**T-Certs** 454

**temporary forks** 180

**Tendermint** 137, 138

- messages 142, 143
- properties 139
- state transition 139
- state variables 143
- usage 140, 141

**Tendermint Core**

- URL 144

**Tessera** 524

**test nets** 282

**test networks**

- connecting to 305

**Tether**

- reference link 45

**Tether gold**

- URL 475

**The Merge** 422-431

- clients 423

**The Open Group Architecture Framework (TOGAF)**

- reference link 510

**The Surge**

- phases 433

- thin block** 205
- threat matrix** 647
- threat modeling** 646, 647
- threshold signatures** 106, 107
- timestamp** 15
- timestamp dependence** 628
- timestamp dependency bugs** 628
- time to live (TTL)** 290
- timing assumptions, consensus algorithm**
  - asynchrony 123
  - partial synchrony 123
  - synchrony 123
- TLS-N-based mechanism** 233
- TLSNotary** 233
- token engineering** 495
  - reference link 496
- tokenization**
  - advantages 470, 471
  - disadvantages 472
  - on blockchain 470
  - process 475, 476
- tokenized blockchains** 25
- tokenless blockchains** 25
- token offerings** 476-478
  - decentralized autonomous initial coin offering 478
  - equity token offerings 477
  - initial coin offerings 476, 477
  - initial exchange offerings 477
  - security token offerings 477
- tokenomics (token economics)** 495
- tokens** 469
  - fungible tokens 473
  - non-fungible tokens (NFTs) 473
  - security tokens 475
  - stable tokens 474
  - taxonomy 496
  - types 473
- token standards** 479
- Token Taxonomy Framework (TTF)** 496
  - reference link 496
- tools, Hyperledger project** 447
  - Caliper 448
  - Cello 448
- Tor** 586
- total order broadcast** 121
- touched accounts** 267
- Town Crier**
  - URL 239
- trade lifecycle**
  - steps 685
- trading instruments** 683
- traditional consensus**
  - properties 146
  - versus Nakamoto consensus 145
- Traditional Finance (TradFi)** 690
- Transact** 444, 447
  - reference link 447
- transaction execution** 266
- transaction families** 445
- transaction flow, Fabric**
  - steps 463, 464
- transaction manager** 524, 527
- transaction order dependence** 630
- transaction ordering dependency bug** 628
- transaction parallelization** 552
- transaction pools** 279
- transaction receipts** 269, 270
- transaction replay attack** 625, 626
- transactions** 16, 255, 264, 279, 458
  - components 257-260
  - contract creation transactions 258, 264
  - message call transactions 258, 265
  - simple transactions 258, 264
- transactions per second (TPS)** 531, 549

**transactions, SegWit**

P2SH-P2WPKH 204

P2SH-P2WSH 204

P2WPKH 203

P2WSH 204

**transaction substate 266****transaction trie 260****transaction validation 266, 277****transparent setups 600****transparent SNARKs 601****Transport Layer Security (TLS) 233, 732****tree chains 558****Trezor**

URL 195

**Triple DES (3DES) 74****TrueBit**

URL 239

**Truffle 351-353, 732**

installing and initializing 392, 393

URL 351

used, for compiling contracts 393-397

used, for deploying with contracts 391, 392

used, for interacting with contracts 391, 392

used, for migrating contracts 393-397

used, for testing contracts 393-397

used, for testing smart contracts 399-404

used, for deploying smart contracts 399-404

**Trusted Execution Environment (TEE) 234, 445, 508, 588****trusted hardware-assisted confidentiality 587****trusted hardware-assisted proofs 235, 236****trusted hardware-assisted scalability 559****trusted model 600****trusted non-universal setup 601****trusted universal setup 601****T-shaped cobbler 722****TumbleBit 590**

phases 590

**tumbler 590****two-phase commit (2PC) 125****two-way peg 209, 557****two-way pegged sidechain 26****tx.origin 630****typical Bitcoin addresses 161, 163****U****UK Jurisdiction Taskforce (UKJT) 224****unauthorized key sharing 637****uncle block 274****unconditional privacy 584****unguarded selfdestruct 629****uniform reference string (URS) 600****Uniform Resource Identifier (URI) 200, 662****unrestricted private transactions 502****unsolvability results 121****Unspent Transaction Output (UTXO) 169, 203****Ursa 444, 447**

reference link 447

**USDT (Tether)**

URL 475

**V****validator node 411, 412**

status 412

**validator nodes**

versus Beacon Chain nodes 414

**validium (validia) 575****Value-Added Tax (VAT) 743****value types 361**

address 362

Boolean 361

- integers 361, 362
- literals 363
- variables, Solidity 359**
  - global variables 359, 360
  - local variables 359
  - state variables 360
- Verifiable Credentials (VCs) 659**
  - architecture, components 660
  - benefits 659
  - ecosystem 662
  - structure 662-664
  - verifiable presentation 665
- Verifiable Data Registries (VDRs) 661, 671**
- verifiable presentation (VP) 665**
- verifiable random function (VRF) 117, 150**
  - URL 150
- view change protocol 132, 133**
- virtual machine 17**
- virtual mining 148**
- virtual read-only memory (virtual ROM) 271**
- Visual Studio Code 353**
- VMware Blockchain (VMBC) 518**
  - architecture 520, 521
  - components 519
  - consensus protocol 519
  - for Ethereum 522
  - reference link 521
- VR headsets 4**
- Vyper 344**
- W**
- Waffle 353**
  - reference link 353
- Wallet Import Format (WIF) 159**
- wallets 289**
- weak collision resistance 56**

- Web3**
  - identity 672-675
  - used, for interacting with contracts 371, 372
- web3.js JavaScript library**
  - installing 382, 383
- web3 object**
  - creating 383
- WebAssembly (Wasm) 272**
- Web evolution, reviewing**
  - Web 1 49
  - Web 2 49
  - Web 3 49
- web layer 48**
- Weierstrass equation 87**
- Whisper 283, 290, 291, 352**
  - reference link 290
- whistleblowing validator 413**
- whitepapers, Hyperledger**
  - reference link 449
- Why3 644**
- Wired Equivalent Privacy (WEP) 636**
- Wireshark**
  - URL 191
- witness 603**
- witnet**
  - URL 239
- world computer 407**
- World of Accountancy 227**
- World of Law 227**
- world state 268**
  - database 457, 458
- world state trie 268**
- X**
- XOR (exclusive OR) 61**

**Y**

yield farming 703

**YUL**

reference link 272

**Z**

**Zcash** 110, 113

URL 21, 111

**zero-knowledge proofs (ZKPs)** 111, 112, 502, 584, 597-601, 737, 741

Ali Baba's Cave analogy 111

challenge phase 113

completeness property 111

response phase 113

soundness property 111

witness phase 113

zero-knowledge property 111

zero-knowledge range proofs (ZKRPs) 116

zk-SNARKs 113-116

**zero-knowledge range proofs (ZKRPs)** 116

**zero-knowledge Succinct Transparent Argument of Knowledge (zk-STARK)** 113, 598

building 601-607

commitment 607

evaluation 608

evaluation proof, verifying 608, 609

limitation 115

proof generation 115

properties 114

setup 607

versus, zk-SNARKs 116

**zero-knowledge (ZK) rollups** 564-566

cons 569

technologies, used for building 566-569

**Zether** 594

**ZK-EVM** 570-572

categories 572

reference link 573

types 572, 573

**Zkledger** 593

**ZKP-related attacks**

attacks on privacy 637

digital signature vulnerabilities 637

inadequate bit security 637

proof malleability 638

quantum threats 637

setup vulnerabilities 638

**ZK-rollups** 575

vs optimistic rollups 573

**zk-SNARK construction**

arithmetic circuit 115

QAP 115

R1CS 115

**ZKSpace** 577

**ZKSwap** 577

**zkSync** 577

**ZK-ZK-rollups** 573

**Zooko's Triangle** 42

# Download a free PDF copy of this book

Thanks for purchasing this book!

Do you like to read on the go but are unable to carry your print books everywhere? Is your eBook purchase not compatible with the device of your choice?

Don't worry, now with every Packt book you get a DRM-free PDF version of that book at no cost.

Read anywhere, any place, on any device. Search, copy, and paste code from your favorite technical books directly into your application.

The perks don't stop there, you can get exclusive access to discounts, newsletters, and great free content in your inbox daily

Follow these simple steps to get the benefits:

1. Scan the QR code or visit the link below



<https://packt.link/free-ebook/9781803241067>

2. Submit your proof of purchase
3. That's it! We'll send your free PDF and other benefits to your email directly



